



Naam dienstonderdeel

BCA, kernteam AFB

-

Datum

16-09-2014

Versienummer

1.1

Opdrachtgever

MT FB

Auteur

Kopie aan

Coördinatie MT FB

Bijlagen

Geen

memo

Voorstel (de)blokkeren IP-adres in het kader van fraudebestrijding

Inleiding.

Er is een bestaande praktijk van het ad-hoc blokkeren van IP-adressen door het SOC (B/CIE). Voor het handmatig blokkeren en deblokkeren wordt om beleid gevraagd. Deze wens is geuit door M1 en B/CIE en beantwoord in de vorm van een opdracht door het MT FB.

Het belang van beleid wordt geschetst aan de hand van de volgende issues en risico's.

Issues.

Er is door 2 teams een opdracht gegeven aan het SOC tot (de)blokkeren:

- 1 Het CAF-team: de casus betrof een ernstig verwarde ex-collega, een exceptionele situatie. Normaliter zal zo'n maatregel niet genomen worden. Deze maatregel is afgestemd met de FIOD. De verwachting is dat dit niet vaker dan 3 keer per jaar kan voorkomen. Recidive zal vervolgens anders aangepakt worden. De opdracht werd door verstrekt aan .
- 2 Toeslagen: Pilot blokkeren IP-adressen van vermoedelijk 'foute' facilitators. Enkele IP-adressen speelden een centrale rol bij het indienen van KOT-verzoeken. De opdracht is zelfstandig en direct aan het SOC verstrekt.

Belastingen en de FIOD hebben aangegeven geen gebruik te maken van het blokkeren, noch daar in de toekomst gebruik van te maken.

De volgende issues zijn op basis van deze schets te onderkennen:

- Wat zijn de omstandigheden voor een verzoek tot het blokkeren van IP-adressen?
- Wat zijn de voorwaarden voor het blokkeren van IP-adressen?
- Wie mag de opdracht verstrekken en aannemen?
- Zijn alle juridische beginselen getoetst?
- Wat zijn de gevolgen in de rechtspositie van de geblokkeerde en eventuele relaties van de geblokkeerde?
- Wat zijn de gevolgen voor de bedrijfscontinuïteit?

Risico's.

- Zonder eenduidig beleid loopt de BD het risico van willekeur.
- Ontbreekt de juridische toets, dan is niet duidelijk of het blokkeren van IP-adressen niet een te zwaarwegend middel is en op de juiste manier is ingezet.
- Het doorlaten van onbetrouwbare berichten is bedreigend voor de continuïteit van de Belastingdienst en vraagt dus om reactie.
- Het stoppen van berichten is mogelijk bedreigend voor de bedrijfscontinuïteit van belanghebbende(n) en hier kan alleen met grote zorgvuldigheid invloed op worden uitgeoefend.
- In de CAF-casus werd ook de ouders van de persoon de mogelijkheid ontnomen om elektronisch aangifte te doen. De vraag is of de geboden alternatieven altijd toepasbaar zijn.

Juridische beschouwing.

Voor alle processen en voorzieningen van de overheid geldt de eis van voorkoming van misbruik en oneigenlijk gebruik, mede gebaseerd op comptabiliteit bij de taakopdracht. De Nationale Ombudsman gebruikt daarvoor de term adequaat, om aan te geven dat zowel het proces als de daarbij vereiste contacten met de burger effectief en efficiënt zijn ingericht.

Bij gebreken aan de betrouwbaarheid en vertrouwelijkheid van een elektronisch bericht (ex afd 2.3 Awb) kan de behandeling worden geweigerd. Waar mogelijk vindt de bekendmaking van de weigeringsbeslissing plaats via de postbus van het gebruikte account onder vermelding van de betreffende logistieke gegevens die herleiding tot het geweigerde bericht mogelijk maken.

Ingevallen waarbij geen retourcommunicatie mogelijk is, kan het gebruik van het kanaal worden beperkt. Hierbij moet een alternatief kanaal beschikbaar zijn voor belanghebbende voor zover het een verplichting betreft of na aanvraag een recht (en daarmee de vereiste van een beslissing op aanvraag) kan worden voorzien.

Aanbevelingen.

Korte termijn aanpak.

Een pragmatische oplossing op korte termijn is om in een bestaand gremium, dat operationeel van aard is en waar de bedrijfsonderdelen in vertegenwoordigd zijn, een afweging te maken of het blokkeren en deblokkeren van IP-adressen per casus het juiste middel is. Het CAF-team komt hiervoor in aanmerking, omdat het tot op heden gaat om facilitators. Voor de volledigheid:

1. Wie willen we aanpakken:

Facilitators die stelselmatig en bij voortduring op elektronische wijze aangiften en verzoeken indienen die gebaseerd zijn op gefingeerde gegevens.

De volgende criteria worden gehanteerd bij de toetsing:

- de aangiften en verzoeken bevatten aantoonbaar gefingeerde gegevens;
- er is een vermoeden van fraude;
- in een eerder stadium is contact met de facilitator niet mogelijk gebleken en/of er wordt door de facilitator niet gehandeld

overeenkomstig de gemaakte afspraken en/of er is sprake van een ernstig verward persoon.

2. Hoe pakken we deze facilitators aan:

De situatie vraagt om snel ingrijpen, derhalve moeten de IP-adressen worden geblokkeerd. Daarmee wordt de stroom mogelijk frauduleuze aangiften/verzoeken stilgelegd.

De vervolgacties zijn mogelijk:

- De facilitator is of wordt aangemeld voor SIS-aanpak, CAF-aanpak en/of strafrechtelijke vervolging.
- De BSN's van de belastingplichtigen die gebruik hebben gemaakt van de facilitator worden signaleerd in AKI (IH) en PIT.
- De aangiften van de facilitator zelf worden opnieuw in onderzoek genomen.

Naast deze acties richting de facilitator worden de frauduleuze aangiften en verzoeken fiscaal gecorrigeerd en de uitbetaalde gelden teruggevorderd bij de belanghebbenden afhankelijk van de omstandigheden.

3. Hoe verloopt het aanmeld- en beslisproces:

Een facilitator kan worden aangemeld door:

- Een medewerker van één de landelijk werkende intelligenceteams (Toeslagen, OB, IH, en kernteam Antifraudebox);
- Ee (regionale) accountmanager van de facilitator;
- Een medewerker van het Combiteam Aanpak Facilitators.

De volgende acties worden vervolgens ondernomen:

- De medewerker stelt een document op waaruit blijkt welke gedragingen van de facilitator ertoe leiden dat het IP-adres moet worden ingetrokken. Daarin moet ook worden vermeld welke acties tot op heden vanuit de Belastingdienst zijn ondernomen om de desbetreffende facilitator weer op het rechte spoor te krijgen. Dit document wordt afgestemd met het CAF team en de M2 CAF.
- De M2 CAF geeft het fiat voor blokkeren.

4. Aanbrengen blokkade.

De desbetreffende facilitator wordt schriftelijk, aangetekend en met redenen omkleedt, geïnformeerd over de blokkade van het IP-adres door een medewerker van het CAF-team.

Voor de uitvoering is direct contact met het SOC afdoende. Het fiat moet dan wel in alle gevallen door de M2 van het CAF gegeven zijn.

5. Deblokkeren.

Op aangeven van de volgende medewerkers kan ook weer worden besloten tot deblokkeren:

- Een medewerker van één de landelijk werkende intelligenceteams (Toeslagen, OB, IH, en kernteam Antifraudebox);
- Ee (regionale) accountmanager van de facilitator;

- Een medewerker van het Combiteam Aanpak Facilitators.

De desbetreffende facilitator wordt schriftelijk over de deblokkade van het IP-adres door een medewerker van het CAF-team.

Voor de uitvoering is direct contact met het SOC afdoende. Het fiat moet dan wel in alle gevallen door de M2 van het CAF gegeven zijn.

Lange termijn aanpak.

Tegelijkertijd kan een start worden gemaakt met een procesbeschrijving in een architectuur. Vanuit die architectuur wordt een juridische analyse (waaronder een PIA) uitgevoerd. Het (de)blokkeren van IP-adressen, maar eventueel ook van andere gegevens, neemt dan als subproces een plek in in deze architectuur. Uitgangspunt is en blijft dat het ontnemen van een bepaalde faciliteit een uiterste noodmaatregel moet zijn. Hiertoe moet een opdracht worden verstrekt.

Het verdient echter nog meer aanbeveling om onderzoek te doen naar mogelijkheden in de toekomst om juist monitoring te gaan verbeteren. Zowel in het kader van het verbeteren van de bedrijfscontinuïteit, als voor de selectieve behandeling van minder betrouwbare berichten. Als voorbeeld dient de aansluiting van Toeslagen op Digipoort met gebruik van PKI Overheid.

Conclusie.

Geconcludeerd kan worden dat het bijhouden van een logging en het gebruik van de verkregen gegevens juridisch motiveerbaar is vanuit meerdere perspectieven. Formeel rechtelijk bestaan geen belemmeringen om de logging bij te houden, de gegevens te gebruiken en in passende gevallen tot weigering van berichten over te gaan. Ook het beperken van het gebruik van het elektronisch kanaal is juridisch motiveerbaar. Ten aanzien van de bedrijfscontinuïteit van de Belastingdienst zullen daartoe logische regels moeten worden geformuleerd. In nader te bepalen gevallen vindt de afhandeling plaats via de inspecteur.

Op korte termijn wordt voorgesteld om het CAF team op te stellen als de verantwoordelijke eenheid die opdrachten geeft voor het (de)blokkeren van IP-adressen, met in achtname van de voorwaarden zoals ze zijn geformuleerd in de aanbevelingen.

Voor een bestendig ingericht proces dient IM ingezet te worden. Voorstel is om het subproces (de)blokkeren van IP-adressen, en wellicht andere gegevens, te integreren in de lopende opdracht die ligt bij IM/BCA, Controle aan de Poort. Dit voorstel ligt ter besluit aan het MT FB.